REMARKS

After the foregoing amendment, claims 32-55 are currently pending in this application. Claims 1-31 have been canceled without prejudice. New claims 32-55 have been added to more distinctly claim subject matter which the applicants regard as the invention. No new matter has been introduced into the application by these amendments.

Claim Rejections - 35 USC § 103

Claims 1-3, 5, 8-13, 18-24, and 28-31 stand rejected under 35 USC § 103(a) as being allegedly unpatentable over Lewis *et al.* (US Patent 6,233,565 B1) in view of Bellwood *et al.* (US Patent 6,584,567 B1). The rejected claims have been canceled, mooting the rejection. Nevertheless, the following remarks are provided in connection with the new claims to advance the prosecution of this application.

The claims are directed to protecting sensitive data stored in a web server environment using a transparent encryption appliance. The appliance identifies sensitive data in a data transaction, encrypts the sensitive data, and replaces the sensitive data with the encrypted sensitive data as the data transaction passes through the appliance, to be stored in the web server environment. In addition, the appliance receives stored encrypted sensitive data in response to a request for corresponding sensitive data, decrypts the received sensitive data, and provides the decrypted sensitive data responsive to the request. Thus, the sensitive data are always encrypted when stored in the web server environment. It is contemplated that the appliance can be used in conjunction with processing electronic commerce (e-commerce) transactions over the Internet, to protect sensitive customer information stored in the server environment.

Web sites often use mechanisms such as the Secure Socket Layer (SSL) protocol to protect sensitive data such as passwords, credit card numbers, and the like, in transit over the Internet between customer computers, e-commerce web servers, and third-party payment processors such as banks. SSL protects data while it is in transit by encrypting it. However, in

the prior art the sensitive data is decrypted when it reaches the web server, which may then store it unencrypted in a server database. As a result, such databases are a prime target of malicious users. The claims ensure that sensitive data is always encrypted before it is stored in such a database. Then, even if a malicious user such as a hacker gains access to the database, the information stored thereon is encrypted and cannot be used by the hacker.

The appliance can also be used to secure web cookies to protect the web server environment against cookies that were altered while stored on a client computer, and to secure passwords stored in the web server environment for use in authenticating password protected actions.

In contrast, Lewis teaches a system for conducting financial transactions involving a client and a server communicating over the Internet, requiring the installation of proprietary software on both the client and the server, and registration and authentication of a user of the system. Lewis also teaches that the server can comprise a server network, and the system can include a third party seller and a third party credit facility for implementing credit card transactions. However, Lewis does not teach the use of an appliance to ensure that sensitive data is encrypted before being stored in the server network. In fact, Lewis teaches a system of just the kind that can benefit from the claims, wherein unencrypted sensitive data can be stored in the server environment thereby rendering the data vulnerable to access and unauthorized use by a malicious user.

As the Examiner notes, Lewis discloses "all purchase and refund requests will be digitally signed and encrypted for transmission from the hosts 10n to the transaction server 180" (Lewis column 14 lines 26-28, emphasis added). However, Lewis does not disclose storing encrypted data. On the contrary, Lewis discloses "After the transaction server 180 receives the purchase request, it interacts with the following servers to execute the transaction: 1. Security server 315 (to verify the user's digital signature and to decrypt the transmitted file) 2. Purchase server 190 (after the purchase request object is deciphered by the transaction server 180, it passes to the purchase server)" (Lewis column 16 line 59 through column 17 line 3, emphasis added).

Thus, transaction data including sensitive information such as a user's password and credit card number are processed and presumably stored unencrypted in MASTER DB 305. The stored data are thus vulnerable to being hacked by a malicious user. In contrast, in accordance with the claims such sensitive information would be protected by encrypting the information before storing it in MASTER DB 305.

Bellwood pertains to extending to an intermediary the privacy of a secure session between a client and one or more so-called origin servers. The intermediary can be a transcoding proxy, required to translate information to be rendered on a so-called pervasive client (such as a web-enabled smartphone) from one source markup language (e.g., HTML) to another (e.g., handheld device markup language (HDML)). Or, the proxy can be for monitoring communications across a firewall, or to take advantage of various services (such as caching) provided by a third party. Bellwood provides a mechanism by which a client in a secure communication session with a data source can provide security information to a proxy to enable the proxy to perform a given function (transcoding, monitoring, caching, etc.) without compromising the security of the secure session. Bellwood does not disclose or suggest encrypting sensitive data using an appliance before it is stored in a web server database, as in the claims.

In particular, with regard to new independent claim 32, claim 32 recites an appliance for protecting data stored in a web server environment, where the web server environment itself does not secure data received from the web before storing it. The appliance is coupled between the server and the network, through which it communicates with clients, and is termed transparent in that the server and network interfaces use the same communications protocol; therefore, the clients and server communicate with each other just as they would without the appliance. A processor of the appliance secures and/or unsecures data. Securing data includes identifying sensitive data received from clients, and encrypting or otherwise securing it before it can be stored in a web server environment. Unsecuring data includes receiving stored secured data, unsecuring it such as by decrypting it, and providing it responsive to a request. Neither Lewis

nor Bellwood, either alone or in any possible combination, teaches or suggests such handling of sensitive data, so that the sensitive data is always secured before it can be stored in a web server environment. Independent claims 44, 53, and 55 are directed system, method, and computer readable medium associated with such an appliance. Claims 43 and 51 are directed to the use of a transparent encryption appliance to protect web cookies against tampering, and claim 52 is directed to the use of secured passwords in conjunction with a transparent encryption appliance for authentication.

Devine pertains to an integrated series of security protocols that protect remote user communications with remote enterprise services, and that protect the enterprise services from third parties. The examiner relies on Devine for providing cookie security. However, Devine does not disclose or suggest an appliance that secures and unsecures web cookies passed between a web server environment that does not secure cookies generated therein and a client, wherein securing the cookie comprises identifying the cookie, securing it by encrypting, hashing, etc., and providing the secured cookie to a client computer, and unsecuring the cookie comprising decrypting or hash verifying, as in the claims. In contrast, Devine at the cited location (Devine column 8 lines 45-60) discloses using a conventional SSL protected communication session, wherein a new cookie is generated "along with each reply to a HTTPS request. The client holds the cookie ... and returns it to the server as part of each subsequent HTTPS request... A new cookie will be generated when the response to the HTTPS request is sent to the client" (Devine column 8 lines 48-57). In other words, Devine teaches that "each session is a single transmission, rather than an interval of time between logon and logoff" (Devine, Abstract).

Because Lewis, Bellwood, and Devine, either alone or in any possible combination, do not disclose or suggest all the elements of the independent claims, those claims are not anticipated by Lewis, Bellwood, or Devine, nor are they obvious in view of Lewis, Bellwood, and/or Devine in any possible combination.

Based on the remarks above, withdrawal of the 35 USC § 103(a) rejection of the claims is respectfully requested.

Conclusion

In view of the foregoing amendment and remarks, applicants respectfully submit that the present application, including claims 32-55, is in condition for allowance and an early notice of allowance is respectfully requested.

Respectfully submitted,

DAN BONEH, *et al.*

BY: 

GREGORY J. LAVORGNA
Registration No. 30,469
DRINKER BIDDLE & REATH LLP
One Logan Square
18th and Cherry Streets
Philadelphia, PA 19103-6996
Tel: 215-988-3309
Fax: 215-988-2757
Attorney for Applicant